Kiteworks

GUIDE

Kiteworks' Implementation of the CISA "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default" Publication

Operationalizing CISA's Vision: Security-by-Design From the Ground Up

Introduction

The goal of the document released by the Cybersecurity and Infrastructure Security Agency (CISA), "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default," is to provide guidance for organizations looking to implement secure design principles in their software development process. The document aims to shift the responsibility of cybersecurity from the customer to the industry, encouraging manufacturers to embrace radical transparency and focus on building safe products. The principles outlined in the document include:

- The burden of safety should never fall solely on the customer and industry needs to take ownership of security outcomes.
- Manufacturers need to embrace radical transparency to disclose and help consumers better understand the scope of consumer safety challenges.
- Tech industry leaders need to focus on building safe products and publish road maps explaining how they will develop and update secure-by-design technology.

The document also emphasizes the importance of incorporating security-by-design and security-by-default principles into the software development process, rather than adding security as an afterthought. By doing so, organizations can reduce the risk of cyberattacks and data breaches, and improve the overall security posture of their products. The principles outlined in the document can also help organizations to comply with relevant regulations and standards related to cybersecurity. In summary, the document provides guidance for organizations looking to improve the security of their software products by incorporating security-by-design and security-by-default principles into their development process. The document aims to shift the responsibility of cybersecurity from the customer to the industry, encouraging manufacturers to embrace radical transparency and focus on building safe products.

The Kiteworks Sensitive Content Tracking, Control, and Protection Platform Enabling a Private Content Network

Kiteworks' FedRAMP and FIPS 140-2 compliant file sharing and governance platform enables organizations to share sensitive information quickly and securely while maintaining full visibility and control over their file-sharing activities. The Kiteworks platform provides:

Secure Software Development

Kiteworks was built using secure software development best practices that align with CISA's "Principles and Approaches for Security-by-Design and Default." Kiteworks enforces least-privilege access, defense in-depth, Secure-by-Default settings, input/output validation, versioning, and industry standards like OWASP and CIS benchmarks.

Secure File Sharing

Kiteworks is FedRAMP Moderate Authorized and enables organizations to access and share data securely, reducing the risk of data breaches, malware attacks, and data loss.

Governance and Compliance

Kiteworks reduces compliance risk and cost by consolidating advanced content governance capabilities into a single platform. Whether employees send and receive content via email, file share, automated file transfer, APIs, or web forms, it's covered.

Simplicity and Ease of Use

Kiteworks enables secure file sharing and collaboration among organizations, individuals, and third-party organizations.

The Kiteworks Platform and CISA "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default" Recommendations for Software Manufacturers

Section: Software Product Security Principles

Technology manufacturers are encouraged to adopt a strategic focus that prioritizes software security. The authoring agencies developed the below three core principles to guide software manufacturers in building software security into their design processes prior to developing, configuring, and shipping their products.

Software Product Security Principles	Kiteworks Supports Compliance	Kiteworks Solution
1. The burden of security should not fall solely on the customer. Software manufacturers should take ownership of the security outcomes of their customer's purchase and evolve their products accordingly.	Yes, supports compliance	Kiteworks was built using secure software development best practices. Kiteworks enforces least-privilege access, defense in-depth, Secure-by-Default settings, input/output validation, versioning, and industry standards like OWASP and CIS benchmarks. Multiple security layers like role-based access, encryption, security reviews, penetration testing, and automated QA defend against threats. Secure coding and validating all inputs/outputs prevent code injection and data loss. Versioning retains file integrity and access to the latest updates. Following these software development and operational principles makes Kiteworks measurably more secure and accountable than the competition. This reduces supply chain risk and meets the enhanced security requirements for federal procurement.

Software Product Security Principles	Kiteworks Supports Compliance	Kiteworks Solution
2. Embrace radical transparency and accountability. Software manufacturers should pride themselves in delivering safe and secure products, as well as differentiating themselves among the rest of the manufacturer community based on their ability to do so. This may include sharing information they learn from their customer deployments, such as the uptake of strong authentication mechanisms by default. It also includes a strong commitment to ensure vulnerability advisories and associated common vulnerability and exposure (CVE) records are complete and accurate. However, beware of the temptation to count CVEs as a negative metric, since such numbers are also a sign of a healthy code analysis and testing community.	Yes, supports compliance	Kiteworks maintains a continuous and extensive cycle of self-testing when it comes to security, conducted by both internal and external researchers and analysts. Internally, all code is tested both manually and automatically during the various SDLC processes. Each new third-party dependency is approved by the security team before going into the final product. The list of third-party components is also regularly compared against the database of known vulnerabilities, and fixes are applied as necessary and published in the release notes. In addition, the Kiteworks code undergoes a full white-hat penetration test conducted by external security experts at least once a year. All Kiteworks products are also made available to the global research community in the form of multiple bug bounty programs. Finally, Kiteworks regularly receives penetration reports from customers. When appropriate, Kiteworks registers and publishes CVEs for vulnerabilities within the products. Kiteworks files CVEs when appropriate, and informs customers of fixed CVEs in each release. In 2024, Kiteworks aims to become a fully registered CVE Numbering Authority (CNA), allowing the ability to maintain and publish official CVEs separately.

Software Product Security Principles	Kiteworks Supports Compliance	Kiteworks Solution
3. Build organizational structure and leadership to achieve these goals. While technical subject matter expertise is critical to product security, senior executives are the primary decision makers for implementing change in an organization. Executive-level commitment for software manufacturers to prioritize security as a critical element of product development requires the development of partnerships with an organization's customers to understand: a. The product deployment scenario guidance along with tailored threat model b. Proposed implementation for security controls to align to Secure-by-Default principles c. Resource allocation strategies tailored to company size and the ability to replace legacy development practices with Secure-by-Design practices d. The need to maintain an open line of communication for feedback internally and externally (e.g., employee and customer feedback) regarding product security issues. Software security should be emphasized in internal forums (e.g., all-hands or brown bags), as well as external product marketing and customer engagement e. Measurements of effectiveness within customer deployments. Senior executive leaders will want to know where investments in security by design and default are helping customers by slowing the pace of security patches, reducing configuration errors, and minimizing attack surface	Yes, supports compliance	a. Kiteworks works closely with customers to understand their deployment scenarios and specific threats, and uses that information to inform its security architecture decisions, test plans, control and setting options, and priorities. b. Kiteworks engineering and product management—supported by the Chief Product Officer, CISO, and CEO—have adopted Secure-by-Default principles as a requirement throughout the product. Kiteworks also employs a dedicated Cyber Security oriented Product Manager, under the title Director of Cyber Security. To protect customers from inadvertent security lapses, the system also warns and requires sign-off on any setting change that is potentially a security or privacy risk. c. Since Kiteworks is a security and compliance product, Secure-by-Design practices are required throughout the development life cycle. d. All software engineers and product managers are trained in the secure development life cycle process, including secure coding practices. Design and code reviews emphasize security. The rest of the employee base is trained in security principles that apply to their roles. Customers can submit security concerns through their Customer Success rep or through Technical Support. Certain issues, such as a penetration test finding, are delivered to the security engineering team to differentiate real vulnerabilities from false positives, advise the customer, and start the process of creating a security fix if needed. Product marketing provides collateral describing important security features for use in the sale cycle. Additionally, Kiteworks posts multiple white papers and technical briefs available on the website and customer portals. e. Kiteworks security engineering tracks rates of vulnerabilities discovered in code reviews, automated testing, internal penetration testing, customer penetration testing, bounty hunters, and customer operations. They regularly make process improvements, including switching or adding penetration test companies and bounty hunters, dramatically improving the number of vulnerabilities discovered and fixed early in the cycle rather than discovered by customers later. Kiteworks' rate of security patches is reported to the CEO monthly. The product reduces customer security configuration errors in two ways. First, security settings are all Secure-by-Default. And second, any potentially risky setting change an admin makes will pop a warning describing the risk, and requiring a sign-off to proceed. It minimizes the attack surface out-of-the-box with its standard hardened virtual appliance.

Software Product Security Principles	Kiteworks Supports Compliance	Kiteworks Solution
Convene routine meetings with company executive leadership to drive the importance of Secure-by-Design and Secure-by-Default within the organization. Policies and procedures should be established to reward production teams that develop products adhering to these principles, which could include awards for implementing outstanding software security practices or incentives for job ladders and promotion criteria.	Yes, supports compliance	Kiteworks hosts a weekly technical meeting where all the latest security concerns, tickets, and initiatives are discussed. This meeting includes the security team, DevOps, and lead developers and engineers. In addition, a monthly security management meeting is held including the CEO, CISO, VP Product, VP Engineering, Director of Cyber Security, and representatives for Customer Support. The security team which is responsible for the security design of the product, including Secure-by-Design and Secure-by-Default, reports regularly to the CEO and executive leadership. Because Kiteworks is a security product, engineers and managers in all areas are expected and incented to use outstanding security practices and designs. As part of every major version release, Kiteworks holds an internal competition between all engineers to find bugs and security issues in the product, including monetary prizes for winners.
Operate around the importance of software security to business success. For example, consider assigning a "software security leader" or a "software security team" that upholds business and IT practices to directly link software security standards and manufacturer accountability. Manufacturers should ensure they have robust, independent product security assessment and evaluation programs for their products.	Yes, supports compliance	Kiteworks' CISO is leading all efforts and responsibilities in maintaining security of the internal IT environment, as well as generally maintaining compliance with all relevant security best practices, standards, and regulations. The CISO leads a cross-functional security team, which closely monitors customer events, evaluates critical corporate and product security decisions, and defines needs to help drive the roadmap of future security features. The Director of Cyber Security is in charge to make sure all of the products are designed and developed according to the highest standards of security, as well as making sure all engineers in the company are developing code according to the security policies and best practices. Automated security testing, regular pen tests, white box analysis, yearly FedRAMP audits, and a bounty program enhance platform security and provide transparency to find vulnerabilities. Kiteworks files CVEs when appropriate, and informs customers of fixed CVEs in each release.

Software Product Security Principles	Kiteworks Supports Compliance	Kiteworks Solution
Use a tailored threat model during development to prioritize the most critical and high-impact products. Threat models consider a product's specific use-case and enable development teams to fortify products. Finally, senior leadership should hold teams accountable for delivering secure products as a key element of product excellence and quality.	Yes, supports compliance	Kiteworks boasts a dedicated threat model that is periodically being reviewed and refined as a joint effort between the security team and the executive level of the company. This threat model is then used as a guide and reference when directing external researchers conducting penetration testing, as well as internal reward structure for the bug bounty programs. Additionally, Kiteworks was built using secure software development best practices. Kiteworks prioritizes defense in-depth, Secure-by-Default settings, input/output validation, and industry standards like OWASP and CIS benchmarks. Multiple security layers like role-based access, encryption, security reviews, penetration testing, and automated QA defend against threats. Secure coding and validating all inputs/outputs prevent code injection and data loss.

Section: Secure-by-Design Tactics

The Secure Software Development Framework (SSDF), also known as National Institute of Standards and Technology's (NIST) SP 800-218, is a core set of high-level secure software development practices that can be integrated into each stage of the software development life cycle (SDLC). Following these practices can help software producers become more effective at finding and removing vulnerabilities in released software, mitigate the potential impact of the exploitation of vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences. The authoring agencies encourage the use of Secure-by-Design tactics, including principles that reference SSDF practices. Software manufacturers should develop a written roadmap to adopt more Secure-by-Design software development practices across their portfolio. The following is a non-exhaustive list of illustrative roadmap best practices:

Secure-by-Design Tactics	Kiteworks Supports Compliance	Kiteworks Solution
Memory safe programming languages (SSDF PW.6.1): Prioritize the use of memory safe languages wherever possible. The authoring agencies acknowledge that other memory specific mitigations, such as address space layout randomization (ASLR), control-flow integrity (CFI), and fuzzing are helpful for legacy codebases, but insufficient to be viewed as Secure-by-Design as they do not adequately prevent exploitation. Some examples of modern memory safe languages include C#, Rust, Ruby, Java, Go, and Swift. Read NSA's memory safety information sheet for more.	Yes, supports compliance	The server-side Kiteworks application is primarily coded in memory safe programming languages outlined in the NSA's memory safety information sheet.

Secure-by-Design Tactics	Kiteworks Supports Compliance	Kiteworks Solution
Secure hardware foundation: Incorporate architectural features that enable fine-grained memory protection, such as those described by Capability Hardware Enhanced RISC Instructions (CHERI) that can extend conventional hardware Instruction-Set Architectures (ISAs). For more information, visit University of Cambridge's CHERI webpage.	Out of Scope	The Kiteworks hardened virtual appliance deploys on customers' VMware and Hyper-V virtualization systems on standard hardware servers the customer provides on their premises. In the cloud, customers can deploy Kiteworks hardened virtual appliances on their leased AWS or Azure resources. Kiteworks also offers a hosting service, with FedRAMP Moderate and IRAP options, all in AWS secure data centers. Additionally, Kiteworks offers FIPS 140-2 support and is in NIST's validation process for 140-3.
Secure software components (SSDF PW 4.1): Acquire and maintain well-secured software components (e.g., software libraries, modules, middleware, frameworks) from verified commercial, open source, and other third-party developers to ensure robust security in consumer software products.	Yes, supports compliance	Libraries incorporated in the product undergo extensive vetting, testing, review, and other techniques. When Kiteworks security engineers find vulnerabilities and fix the code, the company contributes the improvements to the open source community.
Web template frameworks (SSDF PW.5.1): Use web template frameworks that implement automatic escaping of user input to avoid web attacks such as cross-site scripting.	Yes, supports compliance	The Kiteworks design goes beyond web template frameworks: It also embeds a web application firewall (WAF) to identify, alert on, and mitigate a variety of web-bourne attack vectors, as well as signatures of advanced persistent threat activity.
Parameterized queries (SSDF PW 5.1): Use parameterized queries rather than including user input in queries, to avoid SQL injection attacks.	Yes, supports compliance	The Kiteworks product uses parameterized queries and other best practice methods to minimize the opportunities to inject SQL or otherwise run malicious SQL. It also embeds a web application firewall (WAF) that can help identify, alert on, and mitigate SQL injection attacks.

Secure-by-Design Tactics	Kiteworks Supports Compliance	Kiteworks Solution
Static and dynamic application security testing (SAST/DAST) (SSDF PW.7.2, PW.8.2): Use these tools to analyze product source code and application behavior to detect error-prone practices. These tools cover issues ranging from improper management of memory to error prone database query construction (e.g., unescaped user input leading to SQL injection). SAST and DAST tools can be incorporated into development processes and run automatically as part of software development. SAST and DAST should complement other types of testing, such as unit testing and integration testing, to ensure products comply with expected security requirements. When issues are identified, manufacturers should perform root-cause analysis to systemically address vulnerabilities.	Yes, supports compliance	Kiteworks uses an array of security tests, including SAST/DAST, automated security testing, regular pen tests, and a bounty program, to enhance platform security. All programs are measured and regularly improved.
Code review (SSDF PW.7.1, PW.7.2): Strive to ensure that code submitted into products goes through peer review by other developers to ensure higher quality.	Yes, supports compliance	Kiteworks code changes are required to go through a coding and security review with more senior developers. Product Management must also be notified so they can define the customer impact and drive the appropriate customer communications.
Software bill of materials (SBOM) (SSDF PS.3.2, PW.4.1): Incorporate the creation of SBOM3 to provide visibility into the set of software that goes into products. https://www.cisa.gov/sbom	Yes, supports compliance	The software bill of materials is visible in the administrator console to administrators with System Admin privileges.

Secure-by-Design Tactics	Kiteworks Supports Compliance	Kiteworks Solution
Vulnerability disclosure programs (SSDF RV.1.3): Establish vulnerability disclosure programs that allow security researchers to report vulnerabilities and receive legal safe harbor in doing so. As part of this, suppliers should establish processes to determine root causes of discovered vulnerabilities. Such processes should include determining whether adopting any of the Secure-by-Design practices in this document (or other similar practices) would have prevented the introduction of the vulnerability.	Yes, supports compliance	Kiteworks has a thriving and expanding community of bounty hunters who have earned many good bounties for finding vulnerabilities before they reach customers. The Kiteworks security engineering team evaluates each finding, reproduces it, classifies it, and assigns a score using the CVSS (Common Vulnerability Scoring System), which determines the urgency for the fix.
CVE completeness: Ensure that published CVEs include root cause or common weakness enumeration (CWE) to enable industry-wide analysis of software security root causes. While ensuring that every CVE is correct and complete can take extra time, it allows disparate entities to spot industry trends that benefit all manufacturers and customers. For more information on managing vulnerabilities, see CISA's Stakeholder specific SVCC guidance.	Yes, supports compliance	Kiteworks finds more than 94% of vulnerabilities before they reach customers. In the event that a bounty hunter or independent researcher finds a vulnerability in a Kiteworks version running in the field, Kiteworks strives to include the information useful for analysis in the CVE.

Secure-by-Design Tactics	Kiteworks Supports Compliance	Kiteworks Solution
Defense-in-depth: Design infrastructure so that the compromise of a single security control does not result in compromise of the entire system. For example, ensuring that user privileges are narrowly provisioned and access control lists are employed can reduce the impact of a compromised account. Also, software sandboxing techniques can quarantine a vulnerability to limit compromise of an entire application.	Yes, supports compliance	Multi-factor Authentication (MFA): Kiteworks supports MFA, which is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. This adds an extra layer of security to thwart unauthorized users from gaining access to sensitive data even if they have obtained valid user credentials via phishing or other means. The Kiteworks server can integrate with a third-party MFA service using the RADIUS protocol. When a RADIUS server is not available, Kiteworks native MFA can provide the second factor via email or by integrating with an SMS server. Some customers configure Kiteworks settings to use RADIUS MFA inside their corporate intranet, and Kiteworks native MFA on the external internet. Admins can enable user profiles to require Time-based One-time Passwords (TOTP) used by authenticators apps such as Google Authenticator, Microsoft Authenticator, and Authy. Single Sign-on (SSO): Kiteworks supports SSO, a property of access control of multiple related, yet independent, software systems. With this property, a user logs in once and gains access to all systems without being prompted to log in again at each of them. Customers can log into Kiteworks clients using native authentication based on an email address, SSO (SAML or Kerberos), along with LDAP/AD. This enhances security by limiting the potential for human error. Secure Data Storage: Kiteworks uses double encryption, securing data in transit via TLS 1.2 and at rest via 256-bit AES, to prevent unauthorized access during transmission and storage. Secure Data Transmission: Kiteworks uses TLS 1.2 as the default secure cryptographic protocol. This protocol is used for establishing encryption channels over computer networks to ensure data integrity and privacy. Role-based Access Control: Kiteworks uses fine-grained, role-based governance policies to control access to data. This means that users can only access data that they are authorized to view, based on their role within the organization. Integration With Existing Security Infrastructure: Kiteworks can integrate with an organization's existing security infrastructure, including DLP, ATP, SIEM, MDM, SSO, 2FA, MFA, etc. This allows organizations to leverage their existing investment in security and provides an additional layer of protection. Antivirus Scanning: Kiteworks provides a built-in antivirus scanning option through WithSecure and can embed WithSecure Atlant, enabling antivirus scanning of unlimited sized files. All files within the Kiteworks system are scanned for malware on download and upload, providing an additional layer of protection against threats.

Secure-by-Design Tactics	Kiteworks Supports Compliance	Kiteworks Solution
Satisfy Cybersecurity Performance Goals (CPGs): Design products that meet basic security practices. CISA's Cybersecurity Performance Goals outline fundamental, baseline cybersecurity measures organizations should implement. Additionally, for more ways to strengthen your organization's posture, see the UK's Cyber Assessment Framework which shares similarities to CISA's CPGs. If a manufacturer fails to meet the CPGs—such as not requiring phishing-resistant multi-factor authentication for all employees—then they cannot be seen as delivering Secure-by-Design products.	Yes, supports compliance	Kiteworks is designed expressly to make it easier for organizations to conform with the NIST CSF, CISA CPGs, ISO 27001, and other cybersecurity frameworks. Many capabilities, such as encryption in transit and at rest, are embedded. Others, like multi-factor authentication via RADIUS, only need to be connected to your enterprise security component. Sophisticated, role-based controls default to the most secure settings, making it easier for an organization to meet the requirements of the framework.

Section: Secure-by-Default Tactics

In addition to adopting Secure-by-Design development practices, the authoring agencies recommend software manufacturers prioritize Secure-by-Default configurations in their products. These should strive to update products to conform to these practices as they are refreshed. For example:

Secure-by-Default Tactics	Kiteworks Supports Compliance	Kiteworks Solution
Eliminate default passwords: Products should not come with default passwords that are universally shared. To eliminate default passwords, the authoring agencies recommend products require administrators to set a strong password during installation and configuration. ▪ Mandate multi-factor authentication (MFA) for privileged users. We observe that many enterprise deployments are managed by administrators who have not protected their accounts with MFA. Given that administrators are high value targets, products should make MFA opt-out rather than opt-in. Further, the system should regularly prompt the administrator to enroll in MFA until they have successfully enabled it on their account. Netherlands' NCSC has guidance that parallels CISA's. Visit their Mature Authentication Factsheet for more information.	Yes, supports compliance	Multi-factor Authentication (MFA): Kiteworks supports MFA, a security measure that requires users to provide at least two forms of identification before they can access their account. This typically involves something the user knows (like a password), something the user has (like a mobile device to receive a verification code), and/or something the user is (like a fingerprint or other biometric data). The Kiteworks server can integrate with a third-party MFA service using the RADIUS protocol. When a RADIUS server is not available, Kiteworks native MFA can provide the second factor via email or by integrating with an SMS server. Some customers configure Kiteworks settings to use RADIUS MFA inside their corporate intranet, and Kiteworks native MFA on the external internet. Admins can enable user profiles to require Time-based One-time Passwords (TOTP) used by authenticator apps such as Google Authenticator, Microsoft Authenticator, and Authy. This adds an extra layer of security to thwart unauthorized users from gaining access to sensitive data even if they have obtained valid user credentials via phishing or other means. Also, Kiteworks does not have default passwords, and an admin setting can disable the ability for the same password to log in multiple times. Admins can set strong password policies. If required, Kiteworks administrators have the ability to completely abolish password usage, only allowing users to authenticate via SSO or Client Certificates.

Secure-by-Default Tactics	Kiteworks Supports Compliance	Kiteworks Solution
Single sign-on (SSO): IT applications should implement single sign-on technology via modern open standards. Examples include Security Assertion Markup Language (SAML) or OpenID Connect (OIDC.) This capability should be made available by default at no additional cost.	Yes, supports compliance	Single Sign-on (SSO): Kiteworks supports SSO, a property of access control of multiple related, yet independent, software systems. With this property, a user logs in once and gains access to all systems without being prompted to log in again at each of them. Customers can log in to Kiteworks clients using native authentication based on an email address, SSO (SAML or Kerberos), along with LDAP/AD. This not only improves user experience by reducing the number of times users have to enter their credentials, but it also enhances security by limiting the potential for human error. In addition to SSO, Kiteworks also supports Certificate Based Authentication (CBA).
Secure logging: Provide high-quality audit logs to customers at no extra charge. Audit logs are crucial for detecting and escalating potential security incidents. They are also crucial during an investigation of a suspected or confirmed security incident. Consider best practices such as providing easy integration with security information and event management (SIEM) systems with application programming interface (API) access that uses coordinated universal time (UTC), standard time zone formatting, and robust documentation techniques.	Yes, supports compliance	SIEM Integration: Kiteworks integrates with security information and event management (SIEM) systems. SIEM systems provide real-time analysis of security alerts generated by applications and network hardware. Kiteworks continuously feeds log entries to configured syslogs and SIEM systems such as Splunk, LogRhythm, and ArcSight. This integration allows for centralized logging and analysis, making it easier to identify and respond to security incidents. ATP Integration: Kiteworks servers integrate with commercially available advanced threat prevention (ATP) solutions via the ICAP protocol. The Kiteworks ATP module sends incoming content to ATP servers that scan for unknown threats. If malware is detected, it quarantines the file, logs the event, sends notifications to appropriate security operations personnel, and provides CISO dashboard reporting and analytics. This integration with ATP solutions enhances the security of the system by providing an additional layer of protection against advanced threats. Audit Logs: Kiteworks provides detailed audit logs, which track user activity within the system. These logs can be used to identify potential security threats, provide evidence of compliance with regulatory requirements, and assist in the investigation of security incidents. The audit logs capture information such as user login activity, file access and modifications, and system configuration changes.

Secure-by-Default Tactics	Kiteworks Supports Compliance	Kiteworks Solution
Software authorization profile: Software suppliers should provide recommendations on authorized profile roles and their designated use case. Manufacturers should include a visible warning that notifies customers of an increased risk if they deviate from the recommended profile authorization. For example: Medical doctors can view all patient records, but a medical scheduler has limited access to address information required for scheduling appointments.	Yes, supports compliance	Role-based access, permissions, least-privileged defaults. All users are assigned a set of permissions that control access to features and resources. Kiteworks is designed so users are automatically given the least permissions necessary; administrators must explicitly enable elevated permissions.
Forward-looking security over backwards compatibility: Too often, backwards compatible legacy features are included, and often enabled, in products despite causing risks to product security. Prioritize security over backwards compatibility, empowering security teams to remove insecure features even if it means causing breaking changes.	Yes, supports compliance	Kiteworks deprecates obsolete protocols and subsystems on a regular basis. For example, it supports TLS 1.2, but no longer supports the obsolete TLS 1.0 and 1.1 protocols.

Secure-by-Default Tactics	Kiteworks Supports Compliance	Kiteworks Solution
Track and reduce "hardening guide" size: Reduce the size of "hardening guides" produced for products and strive to ensure that the size shrinks over time as new versions of the software are released. Integrate components of the "hardening guide" as the default configuration of the product. The authoring agencies recognize that shortened hardening guides result from ongoing partnership with existing customers and include efforts by many product teams, including user experience (UX).	Yes, supports compliance	Kiteworks is delivered and deployed as a hardened virtual appliance out of the box; the Kiteworks engineering team executes the "hardening guide" so its customers don't have to. It removes unnecessary software, functions, accounts, etc., encrypts the data, and defaults to the most secure settings and configurations. The entire server—OS, database, web server, application code, and so on—uses one-click updates like a smartphone so customers can effortlessly apply the latest updates to manage vulnerabilities. The Kiteworks server embeds a network firewall that only allows role-based admin and end-user access via the web, with no access to the operating system or database. To mitigate advanced threats, the server embeds a web application firewall (WAF) to detect, alert on, and shut down web-based attacks, and many forms of intrusion detection and trip-wires to detect, alert on, and shut down more intrusive activities. Unlike custom hardening performed after installation, the Kiteworks hardened virtual appliance is subjected to multiple internal and external penetration tests per year, as well as white-hat hackers paid a bounty if they find a new vulnerability and penetrate the hardening.
Consider the user experience consequences of security settings: Each new setting increases the cognitive burden on end-users and should be assessed in conjunction with the business benefit it derives. Ideally, a setting should not exist; instead, the most secure setting should be integrated into the product by default. When configuration is necessary, the default option should be broadly secure against common threats.	Yes, supports compliance	Kiteworks strives to achieve the simplest, least error-prone experience possible for both end-users and admins. Admin settings are secure by default, and admins are warned and need to sign off if they choose a potentially risky setting. Duties such as helpdesk and system administrators are segregated, and access to controls is role-based. End-user access controls are nil by default; access to content is by invitation only from an appropriately authorized party. Many settings do not exist because controls are always on: Content in storage and in transit is encrypted by default, with no controls for admins to potentially turn off or on. Some subsystems, such as the Email Protection Gateway (EPG) apply automatic policies that are transparent to end-users—they just send and receive emails as normal while the system determines which to encrypt and which to send in the clear, for example.

Secure-by-Default Tactics	Kiteworks Supports Compliance	Kiteworks Solution
HARDENING VS. LOOSENING GUIDES Hardening guides may result from the lack of product security controls being embedded into a product's architecture from the start of development. Consequently, hardening guides can also be a roadmap for adversaries to pinpoint and exploit insecure features. It is common for many organizations to be unaware of hardening guides, thus they leave their device configuration settings in an insecure posture. An inverted model known as a loosening guide should replace such hardening guides and explain which changes users should make while also listing the resulting security risks. Rather than developing hardening guides that list methods for securing products, the authoring agencies recommend software manufacturers shift to a Secure-by-Default approach by providing loosening guides. These guides explain the business risk of decisions in plain, understandable language, and can raise organizational awareness of risks to malicious cyber intrusions. Security tradeoffs should be determined by the customers' senior executives, balancing security with other business requirements.	Yes, supports compliance	Because the product ships with the most secure posture by default, changes admins make to security settings constitute "loosening." The "loosening guide" is built into the product, because any time an admin picks a setting that is potentially risky, a warning message pops up to explain the risk. The admin has to sign off to continue, so they can't inadvertently pick a risky setting. The Secure-by-Default and hardened virtual appliance strategy is mandated by the CEO, through the CISO and the Chief Product Officer to all development engineers. All Kiteworks executives review the security roadmap on a monthly basis.

Kiteworks

Kiteworks

www.kiteworks.com

November 2023